IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 19-369
	)	
LAFON ELLIS	)	

MOTION TO COMPEL SOFTWARE VERIFICATION MATERIALS

Lafon Ellis seeks an Order compelling specific software verification and validation materials to test the underlying data and basis for probabilistic genotyping software TrueAllele. The request to compel is made pursuant to Mr. Ellis' Constitutional rights, the *Brady* rule, and various rules of federal evidence and procedure. In support Mr. Ellis states the following:

I. INTRODUCTION/BACKGROUND

1. At issue is whether Constitutional principles, the *Brady* rule, and Rule 16, require the government to disclose software verification and validation materials of TrueAllele software in a case where the government intends to utilize TrueAllele software results as evidence of guilt.

2. Mr. Ellis is charged with 18 U.S.C. 922(g)(1) (unlawful gun possession). Because the person who possessed the gun in this case was not apprehended at the scene, and because regular DNA testing failed to connect Mr. Ellis to any of the evidentiary materials in this case[1], including the gun, the government intends to rely on a software program called TrueAllele in order to prove that Mr. Ellis is guilty of illegal gun possession.

3. TrueAllele is a probabilistic genotyping software owned by Cybergenetics. Cybergenetics is a privately owned, for-profit, software company in the business of marketing TrueAllele. That

[1] Regular forensic testing did not produce a match between Mr. Ellis' DNA and anything in the car the government is alleging he was driving.

software purports to interpret DNA mixtures that are too complex and ambiguous for human DNA analysts to resolve.

4. Probabilistic genotyping software, like TrueAllele, refers to the use of "biological modeling, statistical theory, computer algorithms, and probability distributions" to analyze complex DNA samples. Sci. Working Grp. on DNA Analysis Methods, *Guidelines for the Validation of Probabilistic Genotyping Systems* (2015), http://perma.cc/EZ85-22VE. Probabilistic genotyping is a novel, highly criticized, evolving technology for interpreting complex DNA mixtures. In order to analyze complex mixtures of DNA, with three or more contributors, software is necessary, since it performs hundreds of thousands of calculations, which could not conceivably be performed by hand. TrueAllele relies on a what the company considers to be a proprietary blend of variables, data, and formulas, and analysis of which peaks are "real" genetic material, to generate a so-called "likelihood ratio" ("LR"). An LR compares two hypotheses—the likelihood of seeing the evidence given the hypothesis that a suspect is a contributor to the sample, and the likelihood of seeing the evidence given the competing hypothesis that a suspect is not a contributor to the sample.

5. Cybergenetics is not a laboratory, nor a forensic laboratory, nor a crime lab. As a result, Cybergenetics is not subject to any national or international rigorous forensic laboratory standards for the forensic work they sell, nor do they follow standards required in the relevant fields.

6. Accredited forensics laboratories are regularly audited to maintain accredited status. Those audits are conducted by independent parties that make sure the laboratories are complying with external standards and the laboratories' own standard operating procedures. But because it is not a forensic laboratory, Cybergenetics is not subject to any external oversight or auditing. There is no legal or other requirement that it be subject to audits of its work.

7. Cybergenetics is a software company, in the for-profit business of analyzing DNA and selling its program for forensic use. Like forensic laboratories, software engineering has industry standards that apply to software development, including that of probabilistic genotyping software.

8. The President's Council of Advisors on Science and Technology [PCAST] Report[2] from 2016 presented concerns about the scientific validity of probabilistic genotyping because it has not been subjected to the sorts of scientific testing that would be appropriate in their estimation. *See* PCAST, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* 75–83 (2016), https://perma.cc/8DB8-Y6M6.

9. The Defense's expert, Nathaniel Adams—a recognized expert on probabilistic genotyping software in state and federal courts in the United States and internationally in Australia and Canada—explains that "[t]hree forensic DNA organizations have issued guidance for the validation of probabilistic genotyping software: the United States Scientific Working Group on DNA Analysis Methods (SWGDAM) in 2015; the International Society for Forensic Genetics (ISFG) in 2016; and the United Kingdom Forensic Science Regulator (FSR) in 2018. ISFG states, 'International industry standards apply to software validation, verification and test documentation. These standards can be simplified and extrapolated to forensic genetics.' ISFG's guidance cites the Institute of Electrical and Electronics Engineers (IEEE) Standard 1012-2012, *Standard for*

[2] The President's Council of Advisors on Science and Technology ("PCAST") Report was written at the request of then-President Obama to assess several fields of forensic science to strengthen understanding of those fields and clarify the scientific requirements for foundational validity and validity as-applied. PCAST Report, *supra*, at 1, 4–5. PCAST was composed of recognized experts from a number of scientific disciplines, supported by a number of senior legal advisors with significant experience in the interaction between science and the law. *Id.* at vii–ix. In the wake of a 2009 congressionally mandated studied that called into question "the scientific underpinnings of a number of the forensic disciplines routinely used in the criminal justice system," PCAST was tasked with identifying whether "additional steps . . . could usefully be taken on the scientific side to strengthen the forensic-science disciplines and ensure the validity of forensic evidence used in the Nation's legal system". *Id.* at 1.

System and Software Verification and Validation[3] as an example of a relevant existing software standard." *See* Decl. of Nathanial Adams, attached at Exhibit 1. These bodies recommend that, among other things, probabilistic genotyping software be internally verified and validated prior to use, with ISFG and FSR pointing specifically toward software engineering conceptions and standards for verification and validation.

10. Cybergenetics does not claim to subscribe to existing general standards for forensic casework or software development.

11. Cybergenetics has not published any verification and validation studies to demonstrate that TrueAllele meets the requirements of software validation of probabilistic genotyping software. Cybergenetics does not claim to have, nor has provided documentation indicating that is has, constructed, verified, or validated TrueAllele in accordance with any software engineering standard document, either internal or external to Cybergenetics. *See* Exhibit 1, ¶ 9. There is no external auditing of the software development process and the software itself, according to Cybergenetics, is a proprietary trade secret. Thus, it is not clear whether Cybergenetics has complied with any software standards.

12. Mr. Adams writes, "[t]here is very little information publicly available about the development of the TrueAllele® software, including materials requested in the subpoena such as software engineering documentation or the source code." *See* Exhibit 1 ¶ 8.

13. On February 14, 2020, receipt of Rule 16 material was signed. *See* Doc. No. 11.

14. On April 10, 2020, undersigned counsel, in accordance with local rules, sent a 12-page discovery letter to the government seeking additional discoverable materials not previously

[3] Inst. of Elec. & Electronics Eng'rs, *IEEE Std. 1012-2012: IEEE Standard for System and Software Verification and Validation* (2012).

disclosed via email. The majority of the information requested concerned information to test the reliability of TrueAllele by requesting software verification materials in ¶¶ 5-6 of the amended subpoena to Cybergenetics. *See* Doc. No. 36; Amended Subpoena to Cybergenetics *attached as* Exhibit 2.

15. On April 17, 2020, the government, via email, indicated that it did not intend to respond to the letter, but that the government's file is open in this case, and counsel was free to come over and review it. The government added, however, that it thought that it had already sent over everything.

16. On April 28, 2020, undersigned counsel, via email, wrote, "If you have an 'open file' as you stated, please provide me with the discovery information requested in my letter." Within that same email, undersigned counsel requested additional discovery materials related specifically to TrueAllele. The government responded writing, "My file remains open for your review." Undersigned counsel emailed back by providing two different methods of sharing discovery via cloud-based services. The government responded, via email, "I do not intend to send you anything because, as I have already told you, I believe that I have sent you everything from my file. But, I will make my file available for your review."

17. On May 6, 2020, and June 17, 2020, the government made subsequent productions of Rule 16 evidence relating to TrueAllele. Despite these new productions, the following materials, which are items requested in the subpoena sent to Cybergenetics at Doc. No. 36[4], are **still outstanding**:

A. Software development and operating materials, including but not limited to:
   1. Requirements specifications
   2. Design descriptions
   3. Source code, including dependency and build instructions and scripts
   4. The server-side database and executable computing components
   5. All version control system history (e.g. git or SVN)

[4] Exhibit 2.

6. Formal software testing plans, records, or reports have been provided.
7. Issue and bug tracking, including issue reports and change requests
8. Internal and external communications regarding development plans, processes, or requests
9. Change logs
10. All Operating manuals, plans, and procedures, only some were provided were provided.
11. Proficiency tests, including responses, used by personnel involved in validation processes or the instant case
12. Verification and validation plans and reports
13. Qualification and user testing plans and reports, the only validation studies provided were written as articles or reports by Cybergenetics or client labs.
14. Internal software development, quality assurance, and quality control processes, plans, and reports

B. Records and electronic data used or generated by TrueAllele during validation study efforts, and any extant summaries thereof, have only been partially provided. One set of electronic data files has been provided, though records and electronic data files underlying dozens of studies/reports have not been provided.
C. Products of validation study efforts, including proposals, notes, memos, reports, graphics, tables, summaries, conclusions, and any resulting publications, presentations, and reports have been partially provided, mostly by way of complied reports and articles.
D. Biological testing case file
E. Chain of custody and current disposition of evidence
F. Data files created in the course of performing DNA testing and analyzing data
G. Unexpected results and corrective actions reports
H. Job descriptions of Cybergenetics personnel and proficiency test results
I. Verification results
J. Summary of bases relied upon by TrueAllele
K. Written reports relied upon by TrueAllele and person operating TrueAllele
L. Features and limitations of probabilistic genotyping program (TrueAllele) and the impact that those items will have on the validation process
M. All validation studies documented by the lab in accordance with the FBI Quality Assurance Standards for Forensic DNA Testing Laboratories.
N. Proof of appropriate security protection to ensure only authorized users can access the software and data. List of names who accessed the data.

II. POINTS AND AUTHORITIES

Although there is "no general constitutional right to discovery in a criminal case ….,"*Weatherford v. Bursey*, 429 U.S. 545, 559 (1977), as long ago as 1966, a unanimous Supreme Court spoke of "the growing realization that disclosure, rather than suppression, of relevant materials ordinarily promotes the proper administration of criminal justice," and referred to "the expanding body of materials, judicial and otherwise, favoring disclosure in criminal cases analogous to the civil practice." *Dennis v. United States*, 384 U.S. 855, 871, (1966). A few years later, speaking in the context of criminal discovery, the Court observed: "The adversary system of trial is hardly an end to itself; it is not yet a poker game in which players enjoy an absolute right always to conceal their cards until played." *Williams v. Florida*, 399 U.S. 78, 82, (1970). As one leading treatise has opined, "no sound reason has yet been advanced why the fullest discovery is permitted in civil actions involving only money and property, but denied in criminal actions involving liberty and life." 4 Barron, Federal Practice and Procedure, 1951, p. 125.

Contrary to what the government may assert in this case, Mr. Ellis is not seeking to know every piece of evidence in the government's hands. What Mr. Ellis is seeking is access to software verification and validation materials in order to test the reliability of a software algorithm the government is attempting to use which purports to claim that Mr. Ellis' DNA was on a gun found in a car. Access to this information is material to Mr. Ellis' defense and relevant to the determination of the forthcoming motion to exclude and *Daubert*[5] hearing and has a "tendency to make a fact more or less probable than it would be without the evidence." The facts at issue being, among other things, whether the software makes appropriate assumptions and whether or not it was developed in a way that makes it scientifically valid and reliable, which is "of consequence to the action." Fed. R. Evid. 401. Thus, under Fed. R. Evid. 401-402, the materials are relevant for this Court to determine the admissibility of TrueAllele.

The Defense must be allowed to review the software verification and validation materials in order to understand and meaningfully confront the prosecution's key evidence of identity—an

[5] *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 589 (1993).

essential element of their case. Due Process and the Confrontation Clause require disclosure of software verification and validation materials relied upon by the prosecution. Failure to disclose such materials violates Mr. Ellis's Sixth Amendment right to confront the evidence against him.

The government's legal duty to produce information that is helpful or useful – and thus favorable to the defense in this prosecution – must be interpreted and enforced within the legal framework outlined below.

A. Brady and rule 16 place significant disclosure requirements on the prosecution.

Under *Brady* and its progeny "the government must always produce any potentially exculpatory or otherwise favorable evidence without regard to how the withholding of such evidence might be viewed – with the benefit of hindsight – as affecting the outcome of the trial." *United States v. Safavian*, 233 F.R.D. 12, 16 (D.D.C. 2005). Failure to disclose all evidence favorable to the accused that is material on either guilt or sentencing violates due process. *See Kyles v. Whitley*, 514 U.S. 419, 432 (1995). There is no distinction between exculpatory evidence and impeachment evidence for purposes of determining whether evidence is considered 'favorable' for purposes of *Brady*. *See United States v. Bagley*, 473 U.S. 667, 676 (1985).

Evidence is considered 'favorable' if it has a "reasonable probability" to affect the outcome of the case. *Whitley,* 514 U.S. at 435. The focus of the Brady rule is fairness. *See Id*. at 454. The meaning of "favorable" includes any information in the possession of the government that relates to guilt or punishment and tends to help the defense by either bolstering the defense case or impeaching potential prosecution witnesses. *Safavian*, 233 F.R.D. at 16. It covers both exculpatory and impeachment evidence. *United States v. Bagley*, 473 U.S. 667, 676-677 (1985). '"The government is obligated to disclose all evidence relating to guilt or punishment which might be reasonably considered favorable to the defendant's case,' that is, all favorable evidence that is itself admissible or 'that is likely to lead to favorable evidence that would be admissible'. . . ." *Safavian*, 233 F.R.D. at 17 (quoting *United States. v. Sudikoff*, 36 F. Supp. 2d 1196, 1199-1200 (C.D. Cal. 1999)). "Where doubt exists as to the usefulness of the evidence to the defendant, the government must resolve all such doubts in favor of full disclosure." *Safavian*, 33 F.R.D. at 17 (citing *United States v. Paxson*, 861 F.2d 730, 737 (D.C. Cir. 1988)); *see Dennis v. Sec., Pennsylvania Dept. of Corrections*, 834 F.3d 263, 293 (3d Cir. 2016) ("All favorable material ought to be disclosed by the prosecution.").

The government's discovery obligations extend to the "Prosecution Team." A prosecutor has a duty to search for and disclose exculpatory evidence if the evidence is possessed by a person or agency that has been used by the prosecutor or the investigating agency to assist the prosecution or the investigating agency in its work. The important determination is whether the person or agency has been "acting on the government's behalf"' *Whitley,* 514 U.S. at 437.

B. Rule 16 is broader than Brady.

The disclosure required by Rule 16 is broader than that required by the due process standards of *Brady*. *See e.g., United States v. Messerlian*, 832 F.2d 778, 795 (3d Cir. 1987) ("[W]e recognize that the disclosure provision of Rule 16 is arguably broader than the Brady requirement."); *United States v. Conder*, 423 F.2d 904, 911 (6th Cir. 1970) ("[T]he disclosure required by Rule 16 is much broader than that required by the due process standards of Brady.")

Under Rule 16, the requirement for disclosure is not limited to evidence favorable or helpful to the defense, but also encompasses evidence that is helpful to the preparation of a defense by permitting the accused to conduct an investigation (i) to attempt to discredit evidence the government may present and (ii) to avoid presenting evidence that may be undercut by evidence in the possession of the government. "In other words, it is just as important to the preparation of a defense to know its potential pitfalls as it is to know its strengths." *United States v. Marshall*, 132 F.3d 63, 67-68 (D.C. Cir. 1998); *see United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993) (the materiality standard '"is not a heavy burden,' . . . rather, evidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.").

A document or item is material, for purposes of Rule 16, if there is "'some indication that the pretrial disclosure of the disputed evidence would . . . enable [ ] the defendant significantly to alter the quantum of proof in his favor.'" *United States v. Dominguez-Chavez*, EP-07-CR-931 PRM, 2007 WL 2008679, at *1 (W.D. Tex. June 13, 2007) (quoting *United States v. Reeves*, 892 F.2d 1223, 1226 (5th Cir. 1990)). This is not a demanding standard. *See United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993)). If a document or item helps the defendant prepare a defense, it is material. *See United States v. Saleh*, 310-CR-083-L, 2010 WL 2944621, at *2 (N.D. Tex. July 26, 2010) (finding statements of co-defendants to be material in preparing a defense).

C. Timely production required.

Both *Brady* and Rule 16 materials must be turned over in a timely manner. The Third Circuit has long suggested a policy of "prompt compliance" with production of discovery. *See Government of Virgin Islands v. Ruiz*, 495 F.3d 1175, 1179 (3d. Cir. 1974) ("[W]e take the occasion to suggest that a more meticulous attention to the government's discovery obligations under Rule 16 and *Brady v. Maryland* [] is highly desirable…An affirmative policy of prompt compliance would, however, avoid the risk of needlessly causing a mistrial or a reversal."). *See also United States v. Higgs*, 713 F.2d 39, 44 (3d Cir.1983); *United States v. Starusko*, 729 F.2d 256, 261 (3d Cir. 1984) ("longstanding policy of encouraging early production."). In addition, pursuant Local Rules, Rule 16 materials are due at arraignment, or 7 days after a defendant's request. *See* LCrR 16(B).[6]

III. ARGUMENT

A. Mr. Ellis is constitutionally and statutorily entitled to the software verification and validation materials pertaining to TrueAllele because they are crucial to a fair assessment of the government's scientific evidence.

1. Due Process & Confrontation Clause[7]

Due Process and the Confrontation Clause require disclosure of the software verification and validation materials because such information constitutes the underlying facts, data, and is materials relied upon by TrueAllele to provide an opinion in this case. The government is relying on TrueAllele's opinion as evidence for the likelihood of Mr. Ellis' DNA being present on the gun. Defense review of software verification and validation materials are essential to the right to confrontation and a fair resolution of a criminal proceeding. Failure to disclose such materials violates Mr. Ellis' Sixth Amendment right to confront the evidence against him.

The source code dictates the operation of an electronic program and is comprised of letters, numbers, symbols, and punctuation marks that often contain material errors as elementary as a misplaced character or symbol.[8] The code can also reveal which—and precisely how—

[6] LCrR 16(B) states: "Upon a defendant's request, the government shall make available the Rule 16 material at the time of the arraignment. If discovery is not requested by the defendant at the time of the arraignment, the government shall disclose such material within seven (7) days of a defendant's request."

[7] These arguments have been adopted from the Amicus Brief written by the Electronic Frontier Foundation and ACLU of Pennsylvania, attached at Exhibit 3.

[8] *See* Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 Cal. L. Rev. 179, 187 (2017); Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 1994 (2017) (quoting Sergey Bratus et al., *Software on the Witness Stand: What Should It Take for Us to Trust It?, in Trust and Trustworthy Computing* 396, 397 (Alessandro Acquisti et al., eds., 2010))

assumptions are incorporated in the program and their effect on the outputted forensic evidence. Independent public scrutiny and testing is the best—and often only—way to discover such errors.[9] Any deficiencies in the TrueAllele's software used to create the match probability of Mr. Ellis' DNA on the gun that might disprove possession are material to preparing the defense, and thereby subject to disclosure by the government. The Defense must be allowed to review the source code in order to understand and meaningfully confront the prosecution's key evidence of identity—an essential element of their case. Meaningful confrontation of the TrueAllele program test results necessarily depends on the defense's access to and opportunity to review the source code and the assumptions embedded within it.

A fair trial necessitates that the accused to "be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; [and] to have compulsory process for obtaining witnesses in his favor." U.S. Const. amend. VI. The right to confrontation is procedural and cannot be disposed of simply because the evidence appears reliable. *Crawford v. Washington*, 541 U.S. 36, 62 (2004) ("Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty."). The Confrontation Clause's animating concern is "to ensure the reliability of the evidence . . . by subjecting it to rigorous testing." *Maryland v. Craig*, 497 U.S. 836, 845 (1990). The Supreme Court has recognized that this concern applies with full force to forensic evidence. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 313 (2009) (holding that affidavits reporting the results of a forensic analysis of seized drugs are testimonial and subject to the Confrontation Clause); *Bullcoming v. New Mexico*, 564 U.S. 647, 663–64, 666 (2011) (holding that certification on a forensic laboratory

[9] Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DePaul L. Rev. 97 (Fall 2016).

report is testimonial and defendant has a right to confront the specific analyst who made the certification).

In the modern context, black-box technologies like TrueAllele squarely parallels the *ex parte* examinations that motivated the founders to adopt the Confrontation Clause in the first place. Performed at the government's demand, intentionally opaque in its operation, and unduly impressive to the jury, both render the defendant powerless to test the credibility of the source and undermine the state's case against him. One side (the prosecution) would have use of evidence reasonably believed to be essential to a fair resolution of the lawsuit—namely, the program methodology that must be examined for accuracy, functionality and credibility in order to meaningfully confront the test results—which was denied to the opposing party. Thus, disclosure is necessary to ensure that Mr. Ellis receives a "fair trial, understood as a trial resulting in a verdict worthy of confidence." *Kyles v. Whitley*, 514 U.S. 419, 434 (1995). The rights of the accused and the obligations of the government cannot be subjugated by the interest of private businesses in maintaining a purported trade secret and Mr. Ellis is entitled to review the software verification and validation materials, including the source code upon which the prosecution's case relies.

2. Fed. R. Crim. P. Rule 16(a)(1)(E)

Under Rule 16(a)(1)(E) "the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items," if the requested item is "within government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant."

Courts have held that "documents are considered part of the evidence in chief if they are marked and offered into evidence by the government or relied on or referred to in any way by the government's witness." *United States v. Jordan*, 316 F. 3d 1215, 1250 n. 75 (11th Cir. 2003).

In *United States v. Liquid Sugars, Inc.*, 158 F.R.D. 466, 471-472 (E.D. Ca. 1994), the defendant in a Clean Water Act prosecution sought to compel production of documents concerning sampling, testing and underlying analysis of wastewater. The court ordered production of a broad range of items, including chain of custody, laboratory bench sheets, testing procedures utilized, calibration standards utilized, laboratory preparation logs, identifying information for instruments and equipment utilized, and "other methodologies actually employed for the testing," which is identical to much of the same information being requested in the present motion. In interpreting what is now Rule 16(a)(1)(E), the court stated:

> This court defines "material information" for Rule 16(a)(1)(C) purposes as that information, not otherwise provided for or precluded by discovery rules, which is significantly helpful to an understanding of important inculpatory or exculpatory evidence. "'The materiality requirement typically 'is not a heavy burden,' rather, evidence is material as long as there is a strong indication that ... [the evidence] will 'play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.' " United States v. Jackson, 850 F.Supp. 1481, 1503 (D.Kan.1994) quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C.Cir.1993) (emphasis added). **For example, if the government plans to use the results of scientific tests as evidence, data and reports which directly underlie those results are generally important to an understanding of the evidence.**

158 F.R.D. at 471.

In *United States v. W.R. Grace*, 233 F.R.D. 586, 590 (D. Mont. 2005) another defendant in a Clean Water Act, wire fraud, and obstruction of justice prosecution sought to compel production of "documents underlying asbestos sampling tests performed by the government or its experts on the soil and air in the Libby area" because they were material to preparing the defense. *Id*. at 587–88. The Court granted the defenses request writing that: "The reasoning of the Liquid Sugars court is persuasive and will be applied here. The underlying documents that are directly pertinent to an understanding of the asbestos sampling results should be produced because the Defendants have established that those documents meet the requirements for production under Rule 16(a)(1)(E)(i)" 233 F.R.D. at 690.

In *United States v. Siegfried*, 2000 WL 988164 (N.D. III. 2000), chemists from the Drug Enforcement Agency analyzed a number of substances seized from the Siegfried's residence. The government produced the chemists' reports and laboratory notes to the defense. Siegfried then sought discovery of the laboratory protocols--"in other words, testing methodologies-- so that he can have an expert examine them to determine their reliability." The government resisted disclosure of these items, saying that they were outside the scope of then Federal Rule of Criminal Procedure 16(a)(1)(D), which requires production of "results or reports ... of scientific tests or experiments." The district court ruled that

> [B]ased on the limited material now available to the Court, it appears that the government's case will be based in significant part on the results of the tests. That being the case, **considerations of fundamental fairness require that the defense have access to material concerning the manner and means of testing so that it can make an independent determination of the tests' reliability and have a fair opportunity to challenge the government's evidence**. The testing protocols may not be, strictly speaking, "results or reports" of testing and thus may well not be covered by Rule 16(a)(1)(D). Even if not, however, the Court believes for the reasons stated that the protocols are "material to the preparation of the defense" and are thus within the scope of Rule 16(a)(1)(C) even if they are outside the scope of Rule 16(a)(1)(D).

Here, this Court need go no further than Rule 16(a)(1)(E) to decide that the government must allow Mr. Ellis to inspect, copy, or photograph TrueAllele software verification and validation materials. This Court should order production and compel inspection because the government plans to use results of scientific tests (TrueAllele) as evidence, and therefore "data and reports which directly underlie those results are generally important to an understanding of the evidence." *Liquid Sugars, Inc.*, 158 F.R.D. 466 at 471. This Court should follow the reasoning's of *Liquid Sugars*, *W.R. Grace*, *Dioguardi* and *Siegfried* because inspection is needed to prepare for Mr. Ellis' defense.

First, the materials are within the government's possession, custody, or control. The government has control over Cybergenetics because Cybergenetics is working and acting on behalf of the government to analyze DNA samples the government provided them. The government's control over Cybergenetics is logical. Cybergenetics is in the business of selling forensic DNA analysis through their program TrueAllele. The government is utilizing Cybergenetics' products and services as their expert witness for their case in chief against Mr. Ellis. Thus, the government is Cybergenetics employer. As employer, the government has inherent control to request testimony, paperwork, explanations of how TrueAllele works by Cybergenetics staff, and other materials required for Cybergenetics to act on behalf of the government's interests in obtaining a conviction in this case. As a seller of software, Cybergenetics has an interest in providing information necessary to the government to fulfil the government's needs for successful admission of TrueAllele software in federal court. Admission in federal court, will financially benefit Cybergenetics to market their product nationwide. At $40,000 per license, Cybergenetics has a lot to gain if they can successfully be admitted in federal court. Surely, if requested by the government, Cybergenetics would provide the software verification and validation materials. Unless, however, there is a contract between Cybergenetics and the government preventing such materials to be disclosed.[10] Or unless Cybergenetics was hiding something and did not want their flagship product to be independently analyzed and checked by widely accepted software engineering standards.

[10] As part of a subpoena request, the Defense requested any non-disclosure agreement between Cybergenetics and the government.

The materials requested are in the possession, custody, or control of the government as interpreted by the law. Unquestionably, the Cybergenetics is part of the prosecution team. Cybergenetics provided the government with DNA analysis, expert advice, declarations on litigating source code, motions and opinions from other jurisdictions to help litigate legal issues as they arise, expert testimony and a likelihood ratio the government intends to use at trial. Not only does Cybergenetics provide "forensic lab services," they also provide litigation materials to protect both their own and the government's interests in using their software TrueAllele. Thus, not only is Cybergenetics "acting on the government's behalf," in this prosecution, *see Whitley,* 514 U.S. at 437; but, the government is also acting on Cybergenetics behalf by defending Cybergenetics financial, and trade secret interests. *See* Doc. No. 47 at 13-14.

Second, the software verification and validation materials are material to preparing for Mr. Ellis' defense. Mr. Ellis stands accused of a serious felony which he could be imprisoned for a maximum period of 10 years. DNA evidence forms a significant part of the prosecution evidence to the extent that, if inadmissible or distrusted, a conviction would be very hard to obtain. The reliability, accuracy, and trustworthiness of the DNA results produced by TrueAllele software will be challenged in a pre-trial admissibility hearing and in jury trial.

The records sought in this case relate directly to the potential shortcomings of the software because they seek information on instances where the software has failed to perform correctly, failed to perform as expected, or required changes to the code, or which will reveal the circumstances under which the results could be unreliable, inaccurate, imprecise, or otherwise problematic, or because they will describe other limitations of the software. Software quality is best evaluated against objective descriptions with testable pass/fail criteria for measuring compliance with those descriptions. Various methods are used by software developers to ensure and evaluate this compliance, and industry and organizational standards documents set forth frameworks for the tasks that should be undertaken during software conceptualization, construction, maintenance, and use. According to Mr. Adams, three forensic DNA organizations have issued guidance for the validation of probabilistic genotyping software. *See* Exhibit 1 ¶ 10. These bodies recommend, among other things, probabilistic genotyping software be internally verified and validated prior to use. Rigorous independent testing is not merely a best practice for software like TrueAllele. The world's leading computer science review community—IEEE—requires technically, managerially, and financially independent testing for any software where "catastrophic consequences" could result even occasionally. IEEE Standards Ass'n, IEEE Std. 1012-2016: IEEE Standard for System, Software, and Hardware Verification and Validation 196, 199 (2016); *see also* Nathaniel Adams, What Does Software Engineering Have to Do with DNA?, The Champion (May 2018) (discussing importance of subjecting probabilistic genotyping systems to software engineering best practices and independent reviews). The IEEE defines "catastrophic consequences" as "[l]oss of human life, complete mission failure, loss of system security and safety, or extensive financial or social loss." *Id*. at 196. For such software, the IEEE requires that the developer be fully independent from the organization responsible for verifying and validating that the software operates as expected. *Id*. at 199. Unquestionably, being deprived of one's freedom through incarceration is a catastrophic consequences.

Indeed, outside experts have stated that they cannot assess how a probabilistic genotyping system arrives at its answers without access to the source code to verify what the program does. *See* Joe Palazzolo, *Defense Attorneys Demand Closer Look at Software Used to Detect CrimeScene DNA*, Wall St. J. (Nov. 18, 2015), https://on.wsj.com/2ONpnE3. That is because the assumptions the software makes about how to weigh the information analysts put into the algorithm are buried in the source code that Cybergenetics will not share or subject TrueAllele to fully independent review. *See* Andrea Roth, *Trial by Machine*, 104 Geo. L.J. 1245, 1273-74 (2016) (discussing effect of shielding proprietary source code of TrueAllele). Validation studies—which are designed to establish software or devices function as claimed—are insufficient to establish the accuracy of TrueAllele without simultaneous access to the source code because such studies examine only inputs and the outputs produced; they cannot assess how the machine turns those inputs into outputs. Natalie Ram, Innovating Criminal Justice, 112 Nw. U. L. Rev. 659, 688 (2018) (indicating that "reliance on validation studies in place of source code access, rather than alongside it, is likely insufficient to verify that software has performed as its designer claims"). This Court should be weary of the government's staunch defense of a private companies financial interests as a valid argument as to why software verification and validation materials should not be disclosed. The government has openly defended access to software verification materials from being subpoenaed by the defense in motion to quash they wrote on behalf of Cybergenetics. *See* Doc. No. 47. Within that motion, the government chose to champion the cause of Cybergenetics financial interests and trade secret claims in order to prevent the Defense from getting access to software verification and validation materials. *See* Doc. No. 47 at 13-14 (arguing "trade secret" protection and "irreparable financial harm to the company."). In addition, this Court should weary of a software company that purports to opine on the DNA match of a suspect's DNA on a gun in her courtroom without allowing the Defense to inspect its software to make sure it complies with industry standards. What is Cybergenetics hiding? Why are they asking the government to fight tooth and nail to prevent disclosure of industry standards for software verification and validation materials such as their source code? Professor Erin Murphy—a nationally recognized expert in forensic DNA typing whose work has been cited multiple times by the Supreme Court—has argued that obtaining the code itself is crucial in order to fully evaluate TrueAllele. She writes, “Just as courts would not accept opinions from witnesses not shown to have qualifications as an expert, so, too, should courts not accept opinions from digital ‘experts’ without probing the ‘qualifications’ of the technology.”[11]

Third, it is obvious that the government intends to use the results of TrueAllele software in its case-in-chief at trial. Courts have held that items the government says its experts are relying on or referring to in any way are discoverable under Rule 16. *See e.g., United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970)(“We fully agree that the **defendants were entitled to know what operations the computer had been instructed to perform and to have the precise instructions that had been given. It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use on cross-examination if desired.** We place the Government on the clearest possible notice of its obligation to do this and also of the great desirability of making the program and other materials needed for cross-examination of computer witnesses, such as flow-charts used in the preparation of programs, available to the defense a reasonable time before trial.”). Here, Mr. Ellis is entitled to know the internal operations of TrueAllele software in order to test, verify and validate the conclusions it purports to make.

For the reasons set forth above, and the case law interpreting the rule, this Court should mandate disclosure of the software verification and validation materials pursuant Rule 16(a)(1)(E).

3. Fed. R. Crim. P. Rule 16(a)(1)(F)

Under Rule 16(a)(1)(F), the government “must permit a defendant to inspect and to copy or photograph the results or reports of any physical or mental examination and of any scientific

[11] Erin Murphy, *Inside The Cell: The Dark Side Of Forensic DNA* 299 (2015).

test or experiment if: (i) the item is within the government's possession, custody, or control; (ii) the attorney for the government knows--or through due diligence could know--that the item exists; and (iii) the item is material to preparing the defense or the government intends to use the item in its case-in-chief at trial."

In *United States v. Green*, 144 F.R.D. 631, 639 (W.D. N.Y. 1994), the defense sought the results of all physical examinations or scientific tests, as well as the underlying data, including lab notes prepared in connection with such examinations or tests. The government conceded that it had an obligation to turn over the results or reports of scientific tests as specified in Rule 16(a)(1)(D), but otherwise opposed this request. The Court ruled that

> After review of the legal authority cited by defendants, **the government is directed to turn over to the defendants not only all scientific reports but also all findings, scientific or technical data upon which such reports are based.** United States v. Bel-Mar Laboratories, 284 F.Supp. 875, 887 (E.D.N.Y. 1968). Rule 16(a)(1)(C) provides for discovery of documents in the possession of the government "which are material to the preparation of the defendants' defense." Rule 16(a)(1)(D) provides discovery of "any results or reports of physical or mental examinations, and of scientific tests or experiments ... which are within the possession, custody, or control of the government...." These two provisions, when read together, provide ample authority for disclosure of this information ... it would appear to facilitate trial by enabling defense counsel to assess the correctness or sufficiency of the testing and to prepare to cross examine the government's experts and to present defense experts, if appropriate. See United States v. Kelly, 420 F.2d 26, 28 (2d Cir.1969).

Here, this Court should follow the reasoning of *Green*, *Bel-Mar Laboratories*, and *Kelly*, and order disclosure under Rule 16(a)(1)(F). First, as explained above, the software verification and validation materials are within the government's possession, custody, either directly or indirectly through Cybergenetics being part of the prosecution team and "acting on the government's behalf," *see Whitley,* 514 U.S. at 437, to help obtain a conviction in Mr. Ellis' case. Second, the government knows--or through due diligence could know--that the software verification materials exists. The government has already conceded that TrueAllele works based on source code, *see* Doc. No. 47 at 12, and has tried to actively suppress the defense from obtaining those materials from Cybergenetics by acting as their quasi in-house counsel. *See* Doc. No. 47 (government's motion to quash subpoena). Thus, the government knows that the documents and data requested by the defense exist. Rule 16(a)(1)(F) thus provides a second basis upon which this motion for discovery should be granted.

4. Fed. R. Crim. P. Rule 16(a)(1)(G), Rule 2, Fed. R. Evid. 102, 705

Fed.R.Crim.P. 16(a)(1)(G) provides in pertinent part:

> At the defendant's request, the government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial. .... The summary provided under this subparagraph must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications.

According to the Advisory Committee Notes, requiring a summary of the bases relied upon by the expert "should cover not only written and oral reports, tests, reports, and investigations, but any information that might be recognized as a legitimate basis for an opinion under Federal Rule of Evidence 703." This provision was intended to "expand federal criminal discovery" in order to "minimize surprise that often results from unexpected expert testimony, reduce the need for continuances, and to provide the opponent with a fair opportunity to test the merit of the expert's testimony through cross examination." *Id.* Rule 16(a)(1)(G) requires the government to disclose, among other things "the bases and reasons" for an expert's opinion. The committee notes regarding the 1993 Amendments to Federal Rule of Procedure 16 states the following with regarding to the disclosure of the bases for an expert's testimony:

> [w]ithout regard to whether a party would be entitled to the underlying bases for expert testimony under other provisions of Rule 16, the amendment requires a summary of the bases relied upon by the expert. That should cover not only written and oral reports, tests, reports, and investigations, but **any information that might be recognized as a legitimate basis for an opinion** under Federal Rule of Evidence 703, including opinions of other experts.

Notes of Advisory Committee on Rules - 1993 Amendment, Federal Rule of Criminal Procedure 16. (emphasis added). Likewise, the committee note makes clear that Rule 16(a)(1)(G) covers any written and oral reports and any investigations.

In this case, the Allegheny County Forensic Lab analyzed Mr. Ellis' DNA on the gun and found "inconclusive" results. Unable to use that result to their theory of the case at trial, the government turned to Cybergenetics, a for-profit, software company in the business of selling DNA probabilities created by their flagship product TrueAllele. The government's theory of possession in this case hinges on the admissibility of TrueAllele test results. The Defense is seeking software verification and validation materials specifically requested by Mr. Adams, an expert in probabilistic genotyping software, based on software engineering industry standards that apply to software development, including that of probabilistic genotyping software. *See* Exhibit 1. The request is highly technical, specific, and focused to what the industry standards require to test the basis of the ultimate opinion of TrueAllele software. It is undeniable that the government plans to use the results of TrueAllele as evidence in this case and therefore the "data and reports which directly underlie those results are generally important to an understanding of the evidence." *Liquid Sugars, Inc.*, 158 F.R.D. at 471-472. This request is consistent with the government's Rule 16(a)(1)(G) obligations requiring disclosure of the "bases and reasons" for an expert's opinion.

The requested materials are also consistent with Fed. R. Evid. 702 which requires a showing that before an expert's testimony is deemed admissible it must be "based on sufficient facts or data," the "product of reliable principles and methods," and the expert must have "reliably applied the principles and methods to the facts of the case." The software verification and validation materials are relevant and evidentiary because they have a tendency to make a fact more or less probable than it would be without the evidence, and its consequence to determine the validity of and admissibility of TrueAllele. The requested materials help this Court serve her "gatekeeping" role when it comes to expert testimony, "ensur[ing] that any and all scientific testimony or evidence admitted is not only relevant, but reliable." *Daubert*, 509 U.S. at 589. Expert testimony is inadmissible unless it is the "product of reliable principles and methods." Fed. R. Evid. 702(c). Put differently, an ostensibly scientific method like TrueAllele's algorithm for generating likelihood rations is inadmissible unless it is foundationally valid. *Daubert*, 509 U.S. at 593. And the validity can only be scrutinized if the Defense has access to the software verification and validation materials.

The requested material is also consistent with Fed. R. Evid. 705 which requires the expert to "disclose . . . facts or data on cross-examination" which base the opinion the expert gave. *See* Fed. R. Evid. 705. The expert in this case is TrueAllele software, the software verification and validation materials, including source code, are the underlying facts or data contributing to the ultimate opinion. Thus, under Fed. R. Evid. 705 they will ultimately be admissible if this Court finds TrueAllele admissible. Compelling the government to provide records now, is in line with the spirit of the rules and consistent with Fed. R. Evid. 102 which guides this Court's decision-making when dealing with evidence. Rule 102 states, "[t]hese rules should be construed so as to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination." Likewise, early disclosure would be consistent with Fed. R. Crim. P. 2, which tells this Court to interpret the rules in so far as to achieve a "just determination of every criminal proceeding, to secure simplicity in procedure and fairness in administration, and to eliminate unjustifiable expense and delay." *See* Fed. R. Crim. P. 2; *see also Zanfordino*, 833 F. Supp. 429 at

433 ("Inability of a defendant to learn before trial the full basis for an adverse expert opinion would run counter to Fed.R.Cr.P. 2 . . .")

If the government wants to admit TrueAllele's results, it should in all fairness allow Mr. Ellis' expert to examine the software to determine whether industry standards are met and to test its reliability. "Materials relevant to opposing expert testimony involving analysis of evidence fall clearly and squarely within Fed.R.Cr.P. 16(a)(1)(C) if readily available." *Zanfordino*, 833 F. Supp. at 432. Keeping the source code a secret will not help this Court fulfill her obligations to serve as a gatekeeper to this evidence without a full airing of the technical issues, which requires the Defense's expert having access to information the government is trying so hard to prevent being disclosed. An order compelling the software verification and validation materials will fulfill the spirit of the federal rules of evidence by helping to "ascertain[] the truth and securing a just determination." Fed. R. Evid. 102.

The above rules of evidence and procedure thus provide additional statutory support upon which this motion for discovery should be granted.

IV. CONCLUSION

The materials sought in this case are discoverable under Federal Rules of Criminal Procedure and Evidence. As explained above any deficiencies in the TrueAllele's software used to create the match probability of Mr. Ellis' DNA on the gun that might disprove possession are material to preparing the defense and thereby subject to disclosure by the government. These deficiencies would similarly be considered exculpatory, and thereby subject to disclosure under *Brady and Giglio* and therefore mandated by the Fifth and Sixth Amendments to the United States Constitution. Due Process and the Confrontation Clause further mandate production because in all fairness Mr. Ellis should be allowed to look under the hood and confront a machines opinions when that machine has the potential to serve as significant evidence of guilt against him.

Finally, as a necessary concomitant of the forthcoming motion to exclude under *Daubert*, and to the extent this Court finds that Rule 16 does not direct production, this Court is empowered to order production as an appropriate exercise of its inherent authority. *See Degen v. United States*, 517 U.S. 820, 823- 24 (1996)(holding courts "have certain inherent authority to protect their proceedings and judgments in the course of discharging their traditional responsibilities"). Thus, to the extent production is sought as an exercise of this Court's inherent authority, the controversy and secrecy behind Cybergenetics refusal to share software verification and validation materials, and Mr. Adams' experience with inconsistencies generally encountered when conducting forensic software examinations with other probabilistic genotyping systems, provide a sufficient factual basis through which this Court may question whether this software works, and is reliable, as advertised. For the reasons stated above, Mr. Ellis respectfully requests that this Court order the Government to produce:

A. Software development and operating materials, including but not limited to:
    a. Requirements specifications
    b. Design descriptions
    c. Source code, including dependency and build instructions and scripts
    d. The server-side database and executable computing components
    e. All version control system history (e.g. git or SVN)
    f. Formal software testing plans, records, or reports have been provided.
    g. Issue and bug tracking, including issue reports and change requests
    h. Internal and external communications regarding development plans, processes, or requests
    i. Change logs
    j. All Operating manuals, plans, and procedures, only some were provided were provided.
    k. Proficiency tests, including responses, used by personnel involved in validation processes or the instant case
    l. Verification and validation plans and reports
    m. Qualification and user testing plans and reports, the only validation studies provided were written as articles or reports by Cybergenetics or client labs.

n. Internal software development, quality assurance, and quality control processes, plans, and reports

B. Records and electronic data used or generated by TrueAllele during validation study efforts, and any extant summaries thereof, have only been partially provided. One set of electronic data files has been provided, though records and electronic data files underlying dozens of studies/reports have not been provided.

C. Products of validation study efforts, including proposals, notes, memos, reports, graphics, tables, summaries, conclusions, and any resulting publications, presentations, and reports have been partially provided, mostly by way of complied reports and articles.

D. Biological testing case file

E. Chain of custody and current disposition of evidence

F. Data files created in the course of performing DNA testing and analyzing data

G. Unexpected results and corrective actions reports

H. Job descriptions of Cybergenetics personnel and proficiency test results

I. Verification results

J. Summary of bases relied upon by TrueAllele

K. Written reports relied upon by TrueAllele and person operating TrueAllele

L. Features and limitations of probabilistic genotyping program (TrueAllele) and the impact that those items will have on the validation process

M. All validation studies documented by the lab in accordance with the FBI Quality Assurance Standards for Forensic DNA Testing Laboratories.

N. Proof of appropriate security protection to ensure only authorized users can access the software and data. List of names who accessed the data.

Respectfully submitted,

/s/ Khasha Attaran
Khasha Attaran
Assistant Federal Public Defender